Chapter 10
Layer 3 VPN Internet Access Examples

JUNOS software supports Internet access from a Layer 3 virtual private network (VPN). This chapter provides examples that demonstrate how to configure a provider edge (PE) router to provide Internet access to customer edge (CE) routers in a VPN. The method you use depends on the needs and specifications of the individual network. To provide Internet access through a Layer 3 VPN, you need to configure policies on the PE router. You also need to configure the next-table keyword at the [edit routing-instances *routing-instance-name* routing-options static route] hierarchy level. When configured, this statement can point a default route from the VPN table (routing instance) to the main routing table (default instance) inet.0. The main routing table stores all Internet routes and is where final route resolution occurs.

There are several ways to configure a PE router to provide CE routers access to the Internet. These types of access are described in the following sections:

> Non-VRF Internet Access on page 215—Internet and VPN access are separate. The CE routers access the Internet independently of the PE routers.

> Distributed Internet Access on page 216—The PE router provides Internet access to the CE routers. Internet route information is stored in the PE router's main routing table.

> Centralized Internet Access on page 241—Some of the CE routers are specially configured to provide Internet access to the other CE routers within the VPN.

Non-VRF Internet Access

The following sections describe ways to provide Internet access to a CE router in a Layer 3 VPN without using the VPN routing and forwarding (VRF) interface. Because these methods effectively bypass the Layer 3 VPN, they are not discussed in detail.

CE Router Accesses Internet Independently of the PE Router

In this configuration, the PE router does not provide the Internet access. The CE router sends Internet traffic either to another service provider, or to the same service provider but a different router. The PE router handles Layer 3 VPN traffic only (see Figure 27).
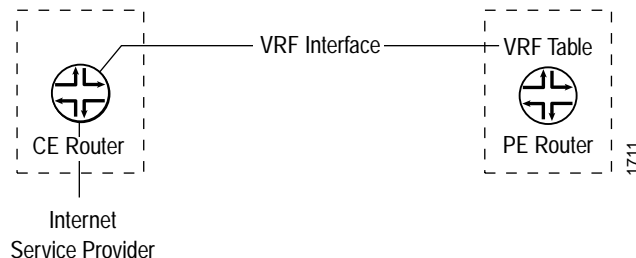
PE Router Provides Layer 2 Internet Service

In this configuration, the PE router acts as a Layer 2 device, providing a Layer 2 connection (such as circuit cross-connect [CCC]) to another router that has a full set of Internet routes. The CE router can use just one physical interface and two logical interfaces to the PE router, or it can use multiple physical interfaces to the PE router (see Figure 28).

Figure 28: PE Router Connects to a Router Connected to the Internet
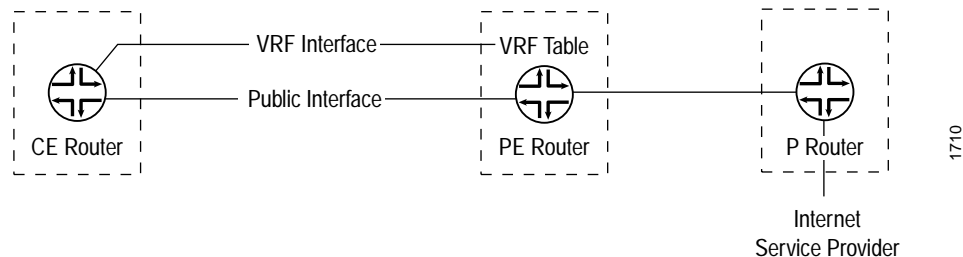
Distributed Internet Access

In this scenario, the PE routers provide Internet access to the CE routers. In the examples that follow, it is assumed that the Internet routes (or defaults) are present in the inet.0 table of the PE routers that provide Internet access to selected CE routers.

When accessing the Internet from a VPN, Network Address Translation (NAT) must be performed between the VPN's private addresses and the public addresses used on the Internet unless the VPN is using the public address space. This section includes several examples of how to provide Internet access for VPNs, most of which require that the CE routers perform the address translation. The "Route Internet Traffic through a Separate NAT Device" example, however, requires that the service provider supply the NAT functionality using a NAT device connected to the PE router.

This section includes the following examples:

In all of the examples, the VPN's public IP address pool (whose entries correspond to the translated private addresses) must be added to the inet.0 table and propagated to the Internet routers to receive reverse traffic from public destinations.

Route VPN and Internet Traffic through Different Interfaces

In this example, VPN and Internet traffic are routed through different interfaces. The CE router sends the VPN traffic through the VPN interface and sends the Internet traffic through a separate interface that is part of the main routing table on Router PE1 (the CE router can use either one physical interface with two logical units or two physical interfaces). NAT also occurs on the CE router (see Figure 29).

Figure 29: Routing VPN and Internet Traffic through Different Interfaces
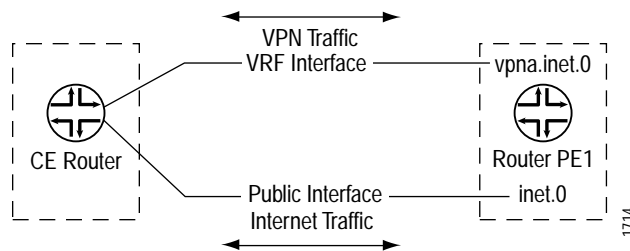
The PE router is configured to install and advertise the public IP address pool for the VPN to other core routers (for return traffic). The VPN traffic is routed normally. Figure 30 illustrates the PE router's VPN configuration.

Figure 30: Example of Internet Traffic Routed through Separate Interfaces
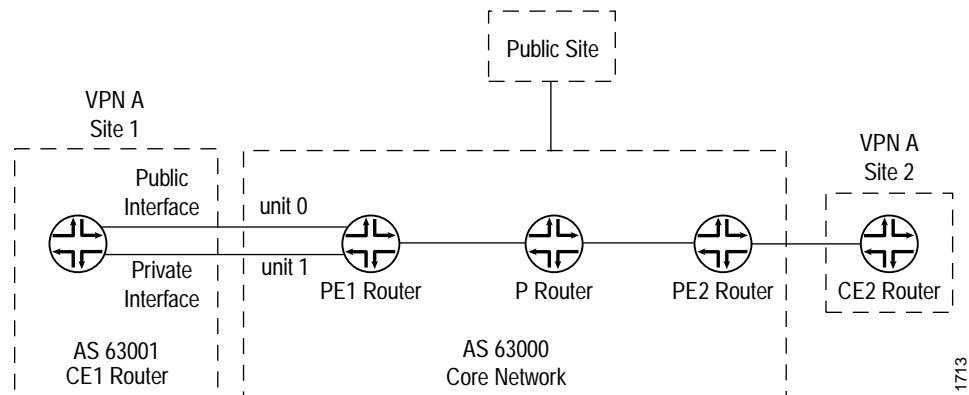
The configuration in this example has the following features:

Router PE1 uses two logical interfaces to connect to Router CE1 using Frame Relay encapsulation.

The routing protocol between Router PE1 and Router CE1 is the external Border Gateway Protocol (EBGP).

Router CE1's public IP address pool is 10.12.1.1-10.12.1.254 (10.12.1.0/24).

The next-hop-self setting is derived from the fix-nh policy statement on Router PE1. PE routers are forced to use next-hop-self so that next-hop resolution is done only for the PE router's loopback address for non-VPN routes (by default, VPN-Internet Protocol version 4 [IPv4] routes are sent using next-hop-self).

You can configure Router CE1 with a static default route pointing to its public interface for everything else.

Configure Interfaces on Router PE1

Configure an interface to handle VPN traffic and an interface to handle Internet traffic as follows:

```
[edit]
interfaces {
    t3-0/2/0 {
        dce;
        encapsulation frame-relay;
        unit 0 {
            description "to CE1 VPN interface";
            dlci 10;
            family inet {
                address 192.168.197.13/30;
            }
        }
        unit 1 {
            description "to CE1 public interface";
            dlci 20;
            family inet {
                address 192.168.198.201/30;
            }
        }
    }
}
```

Configure Routing Options on Router PE1

Configure a static route on Router PE1 to install a route to the CE router's public IP address pool in inet.0 as follows:

```
[edit]
routing-options {
    static {
        route 10.12.1.0/24 next-hop 192.168.198.202;
    }
}
```

Configure BGP, IS-IS, and LDP Protocols on Router PE1

Configure BGP on Router PE1 to allow non-VPN and VPN peering and to advertise the VPN's public IP address pool as follows:

```
[edit]
protocols {
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
                any;
            }
```

```
                  export [ fix-nh redist-static];
                  neighbor 10.255.14.177;
                  neighbor 10.255.14.179;
              }
          }
```

Configure Intermediate System-to-Intermediate System (IS-IS) on Router PE1 to allow access to internal routes as follows:

```
[edit protocols]
   isis {
      level 1 disable;
      interface so-0/0/0.0;
      interface lo0.0;
   }
```

Configure Label Distribution Protocol (LDP) on Router PE1 to tunnel VPN routes as follows:

```
[edit protocols]
   ldp {
      interface so-0/0/0.0;
   }
}
```

Configure a Routing Instance on Router PE1

Configure a routing instance on Router PE1 as follows:

```
[edit]
routing-instances {
   vpna {
      instance-type vrf;
      interface t3-0/2/0.0;
      route-distinguisher 10.255.14.171:100;
      vrf-import vpna-import;
      vrf-export vpna-export;
      protocols {
         bgp {
            group to-CE1 {
               peer-as 63001;
               neighbor 192.168.197.14;
            }
         }
      }
   }
}
```

Configure Policy Options on Router PE1

You need to configure policy options on Router PE1. The fix-nh policy statement sets next-hop-self for all non-VPN routes:

```
[edit]
policy-options {
    policy-statement fix-nh {
        then {
            next-hop self;
        }
    }
}
```

The redist-static policy statement advertises the VPN's public IP address pool:

```
[edit policy-options]
    policy-statement redist-static {
        term a {
            from {
                protocol static;
                route-filter 10.12.1.0/24 exact;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
```

Configure import and export policies for vpna as follows:

```
[edit policy-options]
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-export {
        term a {
            from protocol bgp;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            then reject;
        }
    }
    community vpna-comm members target:63000:100;
}
```

Traffic Routed by Different Interfaces Configuration Summarized by Router

Router PE1

Interfaces
```
interfaces {
    t3-0/2/0 {
        dce;
        encapsulation frame-relay;
        unit 0 {
            description "to CE1 VPN interface";
            dlci 10;
            family inet {
                address 192.168.197.13/30;
            }
        }
        unit 1 {
            description "to CE1 public interface";
            dlci 20;
            family inet {
                address 192.168.198.201/30;
            }
        }
    }
}
```

Routing Options
```
routing-options {
    static {
        route 10.12.1.0/24 next-hop 192.168.198.202;
    }
}
```

BGP Protocol
```
protocols {
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
                any;
            }
            export [ fix-nh redist-static];
            neighbor 10.255.14.177;
            neighbor 10.255.14.179;
        }
    }
```

IS-IS Protocol
```
    isis {
        level 1 disable;
        interface so-0/0/0.0;
        interface lo0.0;
    }
```

LDP Protocol
```
    ldp {
        interface so-0/0/0.0;
    }
}
```
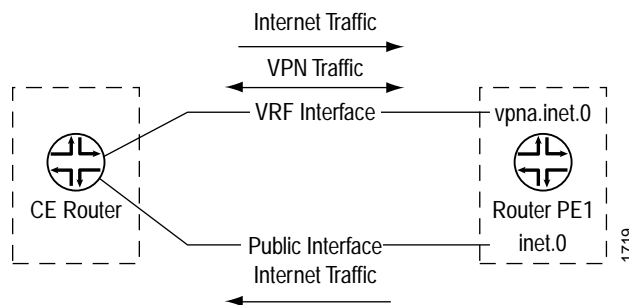
Routing Instance

```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        protocols {
            bgp {
                group to-CE1 {
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Policy Options/Policy Statements

```
policy-options {
    policy-statement fix-nh {
        then {
            next-hop self;
        }
    }
    policy-statement redist-static {
        term a {
            from {
                protocol static;
                route-filter 10.12.1.0/24 exact;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
```

Import and Export Policies

```
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-export {
        term a {
            from protocol bgp;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            then reject;
        }
    }
    community vpna-comm members target:63000:100;
}
```

Route VPN and Outgoing Internet Traffic through the Same Interface and Route Return Internet Traffic through a Different Interface

In this example, the CE sends VPN and Internet traffic through the same interface but receives return Internet traffic through a different interface. The PE router has a default route in the VRF table pointing to the main routing table inet.0. It routes the VPN public IP address pool (return Internet traffic) through a different interface in inet.0 (see Figure 31). The CE router still performs NAT functions.

Figure 31: VPN and Outgoing Internet Traffic Routed through the Same Interface and Return Internet Traffic Routed through a Different Interface

Configuration for Router PE1

This example has the same configuration as Router PE1 in "Route VPN and Internet Traffic through Different Interfaces" on page 217. It uses the topology shown in Figure 30, "Example of Internet Traffic Routed through Separate Interfaces" on page 218. The default route to the VPN routing table is configured differently. At the [edit routing-options] hierarchy level, you configure a default static route that is installed in vpna.inet.0 and points to inet.0 for resolution:

```
[edit routing-options]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-table inet.0;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

You also need to change the configuration of Router CE1 (from the configuration that works with the configuration for Router PE1 described in "Route VPN and Internet Traffic through Different Interfaces" on page 217) to account for the differences in the configuration of the PE routers.

Route VPN and Internet Traffic through the Same Interface Bidirectionally (VPN Has Public Addresses)

This section shows how to configure a single logical interface to handle VPN and Internet traffic traveling both to and from the Internet and the CE router. This interface can handle both VPN and Internet traffic as long as there are no private addresses in the VPN. The VPN routes received from the CE router are added to the main routing table inet.0 using routing table groups. This allows the PE router to attract the return traffic from the Internet (see Figure 32).

Figure 32: Interface Configured to Carry Both Internet and VPN Traffic
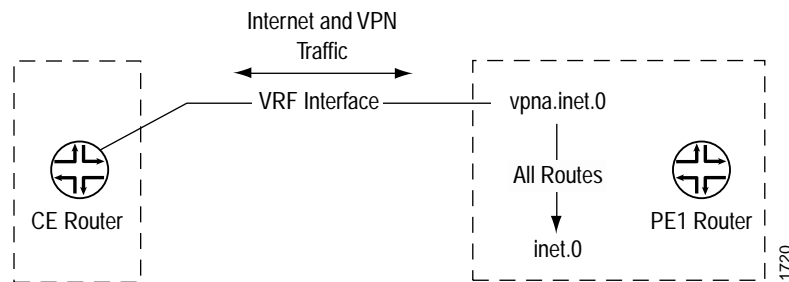
In this example, the CE router does not need to perform NAT because all the VPN routes are public. The CE router has a single interface to the PE router, to which it advertises VPN routes. The PE router has a default route in the VRF table pointing to the main routing table inet.0. The PE router also imports VPN routes received from the CE router into inet.0 using routing table groups.

The following configuration for Router PE1 uses the same topology as in "Route VPN and Internet Traffic through Different Interfaces" on page 217. This configuration uses a single logical interface (instead of two) between Router PE1 and Router CE1.

Configure Routing Options on Router PE1

Configure a routing table group definition for installing VPN routes in routing table groups vpna.inet.0 and inet.0 as follows:

```
[edit]
routing-options {
    rib-groups {
        vpna-to-inet0 {
            import-rib [ vpna.inet.0 inet.0 ];
        }
    }
```

Configure Routing Protocols on Router PE1

Configure the Multiprotocol Label Switching (MPLS), BGP, IS-IS, and LDP protocols on Router PE1. This configuration does not include the policy redist-static statement at the [edit protocols bgp group pe-pe] hierarchy level. The VPN routes are sent directly to IBGP.

Configure BGP on Router PE1 to allow non-VPN and VPN peering, and to advertise the VPN's public IP address pool as follows:

```
[edit]
protocols {
    mpls {
        interface t3-0/2/0.0;
    }
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
            any;
            }
            export fix-nh;
            neighbor 10.255.14.177;
            neighbor 10.255.14.173;
        }
    }
    isis {
        level 1 disable;
        interface so-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface so-0/0/0.0;
    }
}
```

Configure the Routing Instance on Router PE1

This section describes how to configure the routing instance on Router PE1. The static route defined in the routing-options statement directs Internet traffic from the CE router to the inet.0 routing table. The routing table group defined by the rib-group vpna-to-inet0 statement adds the VPN routes to inet.0.

Configure the routing instance on Router PE1 as follows:

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-table inet.0;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    family inet {
                        unicast {
                            rib-group vpna-to-inet0;
                        }
                    }
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Note that you must configure Router CE1 to forward all traffic to Router PE1 using a default route. Alternatively, the default route can be advertised from Router PE1 to Router CE1 with EBGP.

Traffic Routed through the Same Interface Bidirectionally Configuration Summarized by Router

Router PE1

This example uses the same configuration as in "Route VPN and Internet Traffic through Different Interfaces" on page 217. This configuration uses a single logical interface (instead of two) between Router PE1 and Router CE1.

Routing Options
```
routing-options {
    rib-groups {
        vpna-to-inet0 {
            import-rib [ vpna.inet.0 inet.0 ];
        }
    }
}
```

Routing Protocols
```
protocols {
    mpls {
        interface t3-0/2/0.0;
    }
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
            any;
            }
            export fix-nh;
            neighbor 10.255.14.177;
            neighbor 10.255.14.173;
        }
    }
    isis {
        level 1 disable;
        interface so-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface so-0/0/0.0;
    }
}
```

Routing Instance
```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-table inet.0;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    family inet {
                        unicast {
                            rib-group vpna-to-inet0;
                        }
                    }
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Route VPN and Internet Traffic through the Same Interface Bidirectionally (VPN Has Private Addresses)

The example in this section shows how to route VPN and Internet traffic through the same interface in both directions (from the CE router to the Internet and from the Internet to the CE router). The VPN in this example has private addresses. If you can configure EBGP on the CE router, you can configure a PE router using the configuration outlined in "Route VPN and Internet Traffic through the Same Interface Bidirectionally (VPN Has Public Addresses)" on page 225, even if the VPN has private addresses. In the example described in this section, the CE router uses separate communities to advertise its VPN routes and public routes. The PE router selectively imports only the public routes into the inet.0 routing table. This configuration ensures that return traffic from the Internet uses the same interface between the PE and CE routers as that used by VPN traffic going out to public Internet addresses (see Figure 33).

Figure 33: VPN and Internet Traffic Routed through the Same Interface
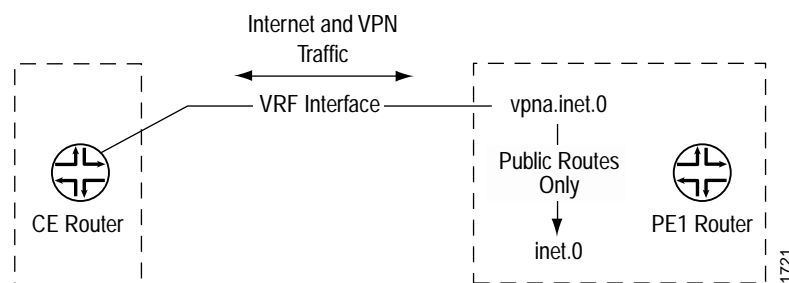
In this example, the CE router has one interface and a BGP session with the PE router, and it tags VPN routes and Internet routes with different communities. The PE router has one interface, selectively imports routes for the VPN's public IP address pool into inet.0, and has a default route in the VRF routing table pointing to inet.0.

Configure Routing Options for Router PE1

On Router PE1, you need to configure a routing table group to install VPN routes in the vpna.inet.0 and inet.0 routing tables:

```
[edit]
routing-options {
    rib-groups {
        vpna-to-inet0 {
            import-rib [ vpna.inet.0 inet.0 ];
        }
    }
}
```

- **Configure a Routing Instance for Router PE1**

On Router PE1, you need to configure a routing instance. As part of the configuration for the routing instance, you need to configure a static route that is installed in vpna.inet.0 and is pointed at inet.0 for resolution.

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-table inet.0;
            }
        }
}
```

At the [edit routing-instances protocols bgp] hierarchy level, configure a policy (import-public-addr-to-inet0) to import public routes into inet.0 and a routing table group (vpna-to-inet0) to allow BGP to install routes into multiple routing tables (vpna.inet.0 and inet.0):

```
[edit routing-instances]
    protocols {
        bgp {
            group to-CE1 {
                import import-public-addr-to-inet0;
                family inet {
                    unicast {
                        rib-group vpna-to-inet0;
                    }
                }
                peer-as 63001;
                neighbor 192.168.197.14;
            }
        }
    }
}
```

Configure Policy Options for Router PE1

Configure the policy options for Router PE1 to accept all routes initially (term a) and then to install routes with a public-comm community into routing table inet.0 (term b):

```
[edit]
policy-options {
    policy-statement import-public-addr-to-inet0 {
        term a {
            from {
                protocol bgp;
                rib vpna.inet.0;
                community [ public-comm private-comm ];
            }
            then accept;
        }
        term b {
            from {
                protocol bgp;
                community public-comm;
            }
            to rib inet.0;
            then accept;
        }
        term c {
            then reject;
        }
    }
    community private-comm members target:1:333;
    community public-comm members target:1:111;
    community vpna-comm members target:63000:100;
}
```

Traffic Routed by the Same Interface Bidirectionally (VPN Has Private Addresses) Configuration Summarized by Router

Router PE1

Routing Options
```
routing-options {
    rib-groups {
        vpna-to-inet0 {
            import-rib [ vpna.inet.0 inet.0 ];
        }
    }
}
```

Routing Instances
```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-table inet.0;
            }
        }
    }
```

Routing Instances Protocols BGP

```
protocols {
    bgp {
        group to-CE1 {
            import import-public-addr-to-inet0;
            family inet {
                unicast {
                    rib-group vpna-to-inet0;
                }
            }
            peer-as 63001;
            neighbor 192.168.197.14;
        }
    }
}
```

Policy Options

```
policy-options {
    policy-statement import-public-addr-to-inet0 {
        term a {
            from {
                protocol bgp;
                rib vpna.inet.0;
                community [ public-comm private-comm ];
            }
            then accept;
        }
        term b {
            from {
                protocol bgp;
                community public-comm;
            }
            to rib inet.0;
            then accept;
        }
        term c {
            then reject;
        }
    }
    community private-comm members target:1:333;
    community public-comm members target:1:111;
    community vpna-comm members target:63000:100;
}
```

Route Internet Traffic through a Separate NAT Device

In this example, the CE router does not perform NAT. It sends both VPN and Internet traffic over the same interface to the PE router. The PE router is connected to a NAT device using two interfaces. One interface is configured in the PE router's VRF table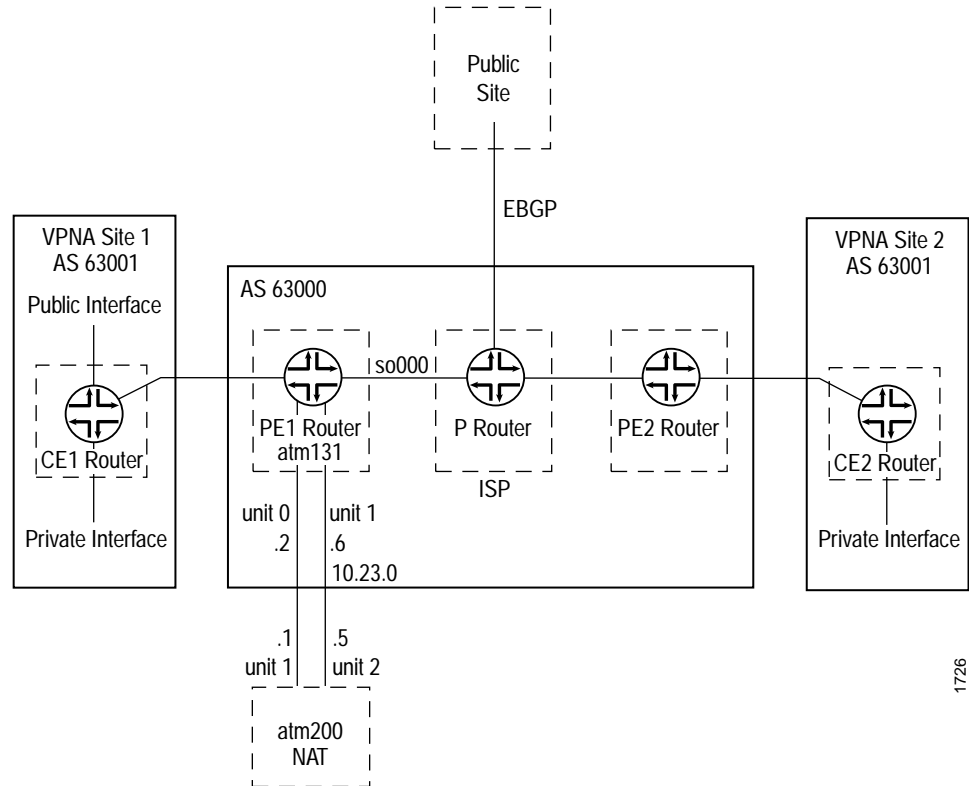 and points to a VPN interface on the NAT device, which can route Internet traffic for the VPN. The other interface is in a default instance, for example, part of public routing table inet.0. There can be a single physical connection between the PE router and the NAT device and multiple logical connections—one for each VRF table and another interface—as part of the global routing table (see Figure 34).

Figure 34: Overview of Internet Traffic Routed through a Separate NAT Device
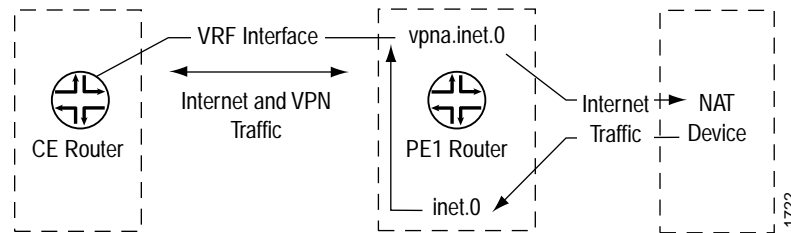
This example's topology expands upon that illustrated in Figure 30 on page 218. The CE router sends both VPN and Internet traffic to Router PE1. VPN traffic is routed based on the VPN routes received by Router PE1. Traffic for everything else is sent to the NAT device using Router PE1's private interface to the NAT device, which then translates the private addresses and sends the traffic back to Router PE1 using that router's public interface (see Figure 35).

Figure 35: Internet Traffic Routed through a Separate NAT Device Example Topology

Public
Site

EBGP

VPNA Site 1
AS 63001

Public Interface

CE1 Router

Private Interface

AS 63000

so000

PE1 Router
atm131

P Router

PE2 Router

ISP

unit 0   unit 1
.2   .6
         10.23.0

.1   .5
unit 1   unit 2

atm200
NAT

VPNA Site 2
AS 63001

CE2 Router

Private Interface

1726

Configure Interfaces on Router PE1

Configure an interface for VPN traffic to and from Router CE1, an interface for VPN traffic to and from the NAT device, and an interface for Internet traffic to and from the NAT device:

```
[edit]
interfaces {
   t3-0/2/0 {
      dce;
      encapsulation frame-relay;
      unit 0 {
         description "to CE1 VPN interface";
         dlci 10;
         family inet {
            address 192.168.197.13/30;
         }
      }
   }
   at-1/3/1 {
      atm-options {
         vpi 1 maximum-vcs 255;
      }
      unit 0 {
         description "to NAT VPN interface";
         vci 1.100;
         family inet {
            address 10.23.0.2/32 {
               destination 10.23.0.1;
            }
         }
      }
      unit 1 {
         description "to NAT public interface";
         vci 1.101;
         family inet {
            address 10.23.0.6/32 {
               destination 10.23.0.5;
            }
         }
      }
   }
}
```

Configure Routing Options for Router PE1

You need to configure a static route on Router PE1 to direct Internet traffic to the CE router through the NAT device. Router PE1 distributes this route to the Internet as follows:

```
[edit]
routing-options {
   static {
      route 10.12.1.0/24 next-hop 10.23.0.5;
   }
}
```

Configure Routing Protocols on Router PE1

Configure MPLS, BGP, IS-IS, and LDP on Router PE1. For the MPLS configuration, include the NAT device's VPN interface in the VRF table. As a part of the BGP configuration, include a policy to advertise the public IP address pool:

```
[edit]
protocols {
    mpls {
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
    }
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
                any;
            }
            export [ fix-nh redist-static ];
            neighbor 10.255.14.177;
            neighbor 10.255.14.173;
        }
    }
    isis {
        level 1 disable;
        interface so-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface so-0/0/0.0;
    }
}
```

Configure a Routing Instance for Router PE1

Configure a routing instance on Router PE1. As part of the routing instance configuration, under routing-options, configure a static default route in vpna.inet.0 pointing to the NAT device's VPN interface (this directs all non-VPN traffic to the NAT device):

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
```

```
            protocols {
                bgp {
                    group to-CE1 {
                        peer-as 63001;
                        neighbor 192.168.197.14;
                    }
                }
            }
        }
    }
    policy-options {
        policy-statement fix-nh {
            then {
                next-hop self;
            }
        }
        policy-statement redist-static {
            term a {
                from {
                    protocol static;
                    route-filter 10.12.1.0/24 exact;
                }
                then accept;
            }
            term b {
                from protocol bgp;
                then accept;
            }
            term c {
                then accept;
            }
        }
        policy-statement vpna-import {
            term a {
                from {
                    protocol bgp;
                    community vpna-comm;
                }
                then accept;
            }
            term b {
                then reject;
            }
        }
        policy-statement vpna-export {
            term a {
                from protocol bgp;
                then {
                    community add vpna-comm;
                    accept;
                }
            }
            term b {
                then reject;
            }
        }
        community vpna-comm members target:63000:100;
    }
```

Traffic Routed by Separate NAT Device Configuration Summarized by Router

Router PE1

Interfaces
```
interfaces {
    t3-0/2/0 {
        dce;
        encapsulation frame-relay;
        unit 0 {
            description "to CE1 VPN interface";
            dlci 10;
            family inet {
                address 192.168.197.13/30;
            }
        }
    }
    at-1/3/1 {
        atm-options {
            vpi 1 maximum-vcs 255;
        }
        unit 0 {
            description "to NAT VPN interface";
            vci 1.100;
            family inet {
                address 10.23.0.2/32 {
                    destination 10.23.0.1;
                }
            }
        }
        unit 1 {
            description "to NAT public interface";
            vci 1.101;
            family inet {
                address 10.23.0.6/32 {
                    destination 10.23.0.5;
                }
            }
        }
    }
}
```

Routing Options
```
routing-options {
    static {
        route 10.12.1.0/24 next-hop 10.23.0.5;
    }
}
```

Routing Protocols

```
protocols {
    mpls {
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
    }
    bgp {
        group pe-pe {
            type internal;
            local-address 10.255.14.171;
            family inet {
                any;
            }
            family inet-vpn {
                any;
            }
            export [ fix-nh redist-static ];
            neighbor 10.255.14.177;
            neighbor 10.255.14.173;
        }
    }
    isis {
        level 1 disable;
        interface so-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface so-0/0/0.0;
    }
}
```

Routing Instance

```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Policy Options
```
policy-options {
    policy-statement fix-nh {
        then {
            next-hop self;
        }
    }
    policy-statement redist-static {
        term a {
            from {
                protocol static;
                route-filter 10.12.1.0/24 exact;
            }
            then accept;
        }
        term b {
            from protocol bgp;
            then accept;
        }
        term c {
            then accept;
        }
    }
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-export {
        term a {
            from protocol bgp;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            then reject;
        }
    }
    community vpna-comm members target:63000:100;
}
```

Centralized Internet Access

This section describes several ways to configure a CE router to act as a central site for Internet access. Internet traffic from other sites (CE routers) is routed to the hub CE router (which also performs NAT) using its VPN interface. The hub CE router then forwards the traffic to a PE router connected to the Internet through another interface identified in the inet.0 table. The hub CE router can advertise a default route to the spoke CE routers. The disadvantage of this type of configuration is that all traffic has to go through the central CE router before going to the Internet, causing network delays if this router receives too much traffic. However, in a corporate network, traffic might have to be routed to a central site because most corporate networks separate the VPN from the Internet by means of a single firewall.

This section includes the following examples:

Route Internet Traffic through a Hub CE Router on page 241

Route Internet Traffic through Multiple CE Routers on page 245

Route Internet Traffic through a Hub CE Router

In this example, Internet traffic is routed through a hub CE router. The hub CE router has two interfaces to the hub PE router: a VPN interface and a public interface. It performs NAT on traffic forwarded from the hub PE router through the VPN interface and forwards that traffic from its public interface back to the hub PE router. The hub PE router has a static default route in its VRF table pointing to the hub CE router's VPN interface. It announces this default route to the rest of the VPN, attracting all non-VPN traffic to the hub CE route. The hub PE router also installs and distributes the VPN's public IP address space (see Figure 36).

Figure 36: Internet Access through a Hub CE Router Performing NAT
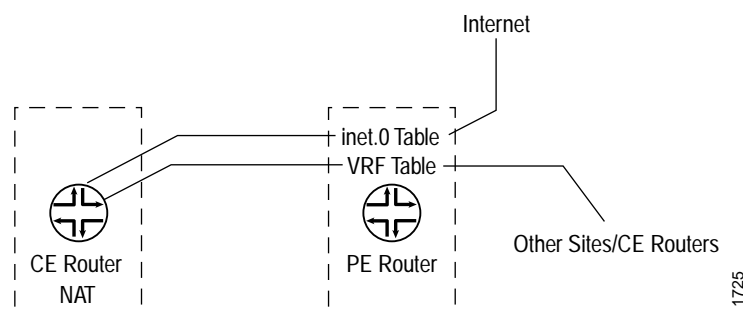
The configuration for this example is almost identical to that described in "Route Internet Traffic through a Separate NAT Device" on page 233. The difference is that Router PE1 is configured to announce a static default route to the other CE routers (see Figure 37).

Figure 37: Internet Access Provided through a Hub CE Router
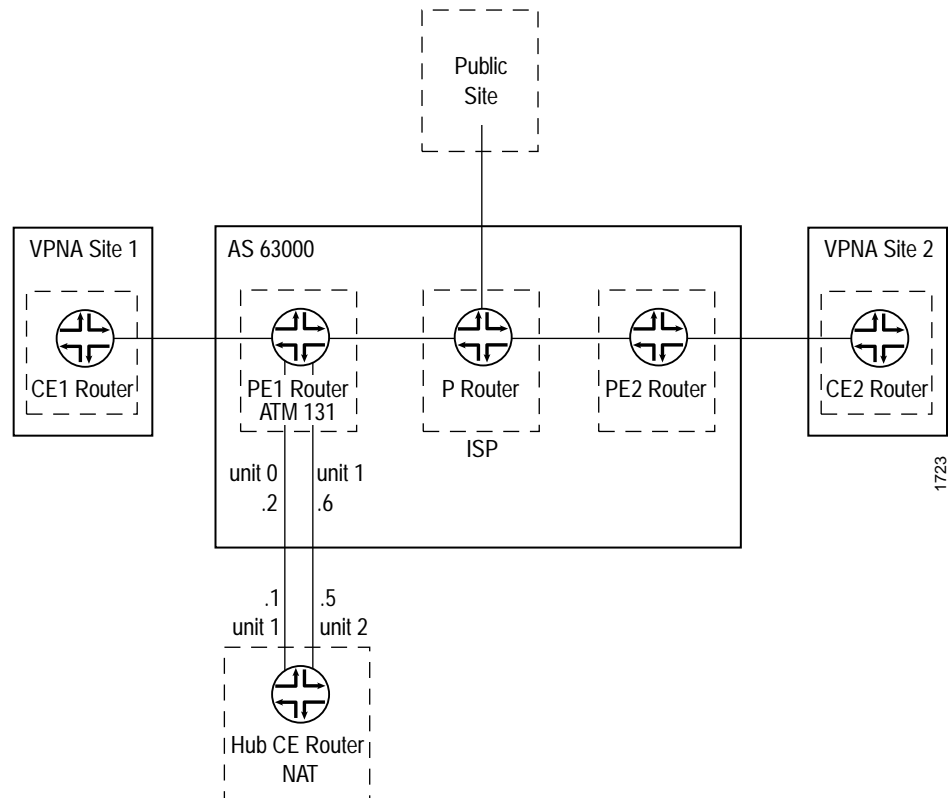
Configure a Routing Instance on Router PE1

Configure a routing instance for Router PE1. As part of this configuration, under routing-options, configure a default static route (route 0.0.0.0/0) to be installed in vpna.inet.0 and point the route to the hub CE router's VPN interface (10.23.0.1). Also, configure BGP under the routing instance to export the default route to the local CE router:

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
```

```
                                    protocols {
                                        bgp {
                                            group to-CE1 {
                                                export export-default;
                                                peer-as 63001;
                                                neighbor 192.168.197.14;
                                            }
                                        }
                                    }
                                }
                            }
                        }
```

Configure Policy Options on Router PE1

Configure policy options on Router PE1. As part of this configuration, Router PE1 should export the static default route to all the remote PE routers in vpna (configured in the policy-statement vpna-export statement under term b):

```
                    [edit]
                    policy-options {
                        policy-statement vpna-export {
                            term a {
                                from protocol bgp;
                                then {
                                    community add vpna-comm;
                                    accept;
                                }
                            }
                            term b {
                                from {
                                    protocol static;
                                    route-filter 0.0.0.0/0 exact;
                                }
                                then {
                                    community add vpna-comm;
                                    accept;
                                }
                            }
                            term c {
                                then reject;
                            }
                        }
                        policy-statement export-default {
                            term a {
                                from {
                                    protocol static;
                                    route-filter 0.0.0.0/0 exact;
                                }
                                then accept;
                            }
                            term b {
                                from protocol bgp;
                                then accept;
                            }
                            term c {
                                then reject;
                            }
                        }
                    }
```

Internet Traffic Routed by a Hub CE Router
Configuration Summarized by Router

Router PE1

The configuration for Router PE1 is almost identical to that for the example in "Route Internet Traffic through a Separate NAT Device" on page 233. The difference is that Router PE1 is configured to announce a static default route to the other CE routers.

Routing Instance
```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    export export-default;
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Policy Options
```
policy-options {
    policy-statement vpna-export {
        term a {
            from protocol bgp;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            from {
                protocol static;
                route-filter 0.0.0.0/0 exact;
            }
            then {
                community add vpna-comm;
                accept;
            }
        }
        term c {
            then reject;
        }
    }
```

```
policy-statement export-default {
    term a {
        from {
            protocol static;
            route-filter 0.0.0.0/0 exact;
        }
        then accept;
    }
    term b {
        from protocol bgp;
        then accept;
    }
    term c {
        then reject;
    }
}
}
```

Route Internet Traffic through Multiple CE Routers

The example in this section is an extension of that described in "Route Internet Traffic through a Hub CE Router" on page 241. This example provides different exit points for different sites by using multiple hub CE routers performing similar functions. Each hub CE router tags the default route with a different route target and allows the spoke CE routers to select the hub site that should be used for Internet access (see Figure 38).

This example uses two hub CE routers that handle NAT and Internet traffic:

Hub1 CE router tags 0/0 with community public-comm1 (target: 1:111)

Hub2 CE router tags 0/0 with community public-comm2 (target: 1:112)

Note that the spoke CE router in this example is configured to have a bias toward Hub2 for Internet access.

Figure 38: Two Hub CE Routers Handling Internet Traffic and NAT
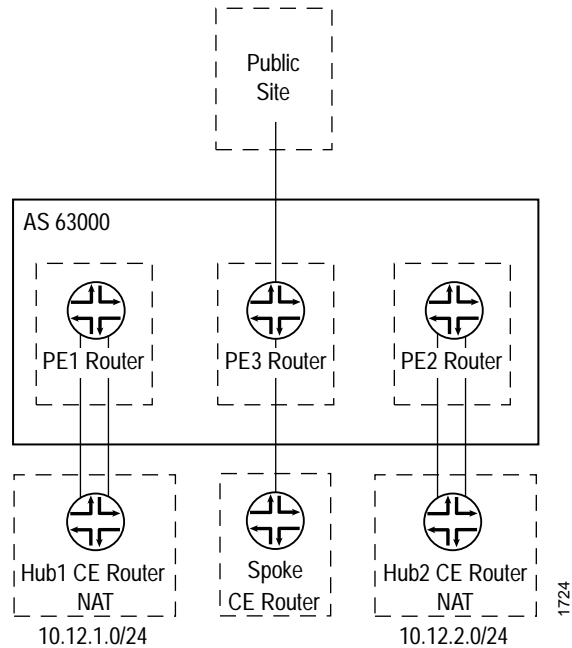
Configure a Routing Instance on Router PE1

Configure a routing instance on Router PE1 as follows:

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    export export-default;
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Configure Policy Options on Router PE1

The policy options for Router PE1 are the same as in "Route Internet Traffic through a Hub CE Router" on page 241, but the configuration in this example includes an additional community, public-comm1, in the export statement:

```
[edit]
policy-options {
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-export {
        term a {
            from {
                protocol static;
                route-filter 0.0.0.0/0 exact;
            }
            then {
                community add public-comm1;
                community add vpna-comm;
                accept;
            }
        }
        term b {
            from protocol bgp;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term c {
            then reject;
        }
    }
    community public-comm1 members target:1:111;
    community public-comm2 members target:1:112;
    community vpna-comm members target:63000:100;
}
```

Note that the configuration of Router PE2 is the identical to that of Router PE1 except that Router PE2 exports the default route through community public-comm2.

Configure a Routing Instance on Router PE3

Configure routing instance vpna on Router PE3 as follows:

```
[edit]
routing-instances {
    vpna {
        instance-type vrf;
        interface t1-0/2/0.0;
        route-distinguisher 10.255.14.173:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        protocols {
            rip {
                group to-vpn12 {
                    export export-CE;
                    neighbor t1-0/2/0.0;
                }
            }
        }
    }
}
```

Configure Policy Options on Router PE3

The vrf-import policy for Router PE3 is configured to select the Internet exit point based on the additional communities specified in "Configure Policy Options on Router PE1" on page 247:

```
[edit]
policy-options {
    policy-statement vpna-export {
        term a {
            from protocol rip;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community public-comm1;
                route-filter 0.0.0.0/0 exact;
            }
            then reject;
        }
        term b {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
```

```
            term c {
                then reject;
            }
        }
        policy-statement export-CE {
            from protocol bgp;
            then accept;
        }
        community vpna-comm members target:69:100;
        community public-comm1 members target:1:111;
        community public-comm2 members target:1:112;
    }
```

Route Internet Traffic through Multiple CE Routers Configuration Summarized by Router

Router PE1

This configuration is an extension of the example in "Route Internet Traffic through a Hub CE Router" on page 241. It provides different exit points for various sites by using multiple hub CE routers that perform similar functions.

Routing Instance
```
routing-instances {
    vpna {
        instance-type vrf;
        interface t3-0/2/0.0;
        interface at-1/3/1.0;
        route-distinguisher 10.255.14.171:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 10.23.0.1;
            }
        }
        protocols {
            bgp {
                group to-CE1 {
                    export export-default;
                    peer-as 63001;
                    neighbor 192.168.197.14;
                }
            }
        }
    }
}
```

Policy Options
```
policy-options {
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term b {
            then reject;
        }
    }
```

```
policy-statement vpna-export {
    term a {
        from {
            protocol static;
            route-filter 0.0.0.0/0 exact;
        }
        then {
            community add public-comm1;
            community add vpna-comm;
            accept;
        }
    }
    term b {
        from protocol bgp;
        then {
            community add vpna-comm;
            accept;
        }
    }
    term c {
        then reject;
    }
}
community public-comm1 members target:1:111;
community public-comm2 members target:1:112;
community vpna-comm members target:63000:100;
}
```

Router PE2

The configuration of Router PE2 is the identical to that of Router PE1, except that Router PE2 exports the default route through community public-comm2 (see "Policy Options" on page 249).

Router PE3

Routing Instances
```
routing-instances {
    vpna {
        instance-type vrf;
        interface t1-0/2/0.0;
        route-distinguisher 10.255.14.173:100;
        vrf-import vpna-import;
        vrf-export vpna-export;
        protocols {
            rip {
                group to-vpn12 {
                    export export-CE;
                    neighbor t1-0/2/0.0;
                }
            }
        }
    }
}
```

Policy Options

```
policy-options {
    policy-statement vpna-export {
        term a {
            from protocol rip;
            then {
                community add vpna-comm;
                accept;
            }
        }
        term b {
            then reject;
        }
    }
    policy-statement vpna-import {
        term a {
            from {
                protocol bgp;
                community public-comm1;
                route-filter 0.0.0.0/0 exact;
            }
            then reject;
        }
        term b {
            from {
                protocol bgp;
                community vpna-comm;
            }
            then accept;
        }
        term c {
            then reject;
        }
    }
    policy-statement export-CE {
        from protocol bgp;
        then accept;
    }
    community vpna-comm members target:69:100;
    community public-comm1 members target:1:111;
    community public-comm2 members target:1:112;
}
```